5th JUNE 2018

SHA-256 MIGRATION ADVISORY

Many organizations need to upgrade to SHA-2 certificates, also known as SHA-256, urgently to meet updated federal and PCI compliance standards and the SHA-1 deprecation policies set by Microsoft, Mozilla, Google and other internet browsers.

SHA-1 has been in use among commercial certification authorities (CAs) since the late 1990s but has been deprecated since November 2013. Recent advances in cryptographic attacks upon SHA-1 have led to the decision that the industry must prohibit continued issuance of SHA-1, but also transition to SHA-2 certificates, which are exponentially more secure. With SHA-2 certificates now available and widely supported by browsers and servers, and the technical deadline for replacement fast approaching, organizations need to maintain their migration path and process to ensure that there are no service disruptions or compromises of their security posture.

Please contact our Customer Support at customercare@digicert.com.my to enquire on the SHA-2 test certificates to enable you to conduct testing on your internal applications to ensure a smooth SHA-256 Migration. If your application is SHA-256 ready, please visit our website at to download your latest root and intermediate certificates which is SHA256 compliant.

Alternatively, if your applications are not ready for the SHA-256 upgrade, you may download the latest SHA-1 (2048) intermediate certificate to ensure uninterrupted service.

The download link is https://www.posdigicert.com.my/downloadpage/root-certificate.

*****END****

Pos Digicert Sdn Bhd **(457608-K)**
CA License No.: LPBP-1/2015(3)

No. 8-3A-02, Star Central,
Lingkaran Cyberpoint Timur,
63000 Cyberjaya,
Selangor Darul Ehsan

+603 – 8800 6000 | www.posdigicert.com.my